



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,905	07/25/2001	Michael L. Wenocur	A-70555/RMA	5467

7590 01/05/2005

FLEHR HOHBACH TEST ALBRITTON & HERBERT LLP
Suite 3400
Four Embarcadero Center
San Francisco, CA 94111-4187

EXAMINER

NGUYEN, MINH DIEU T

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 01/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Applicant No.	Applicant(s)	
	09/912,905	WENOCUR ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 25 July 2001.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1,2,4,13,15,18, 22 and 24 is/are rejected.
- 7) Claim(s) 3,5-12,14,16,17,19-21 and 23 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 10 July 2001 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All
 - b) Some *
 - c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____.
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>01082002, 02122002</u>	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____.

DETAILED ACTION

1. Claims 1-24 are pending.

Specification

2. The disclosure is objected to because of the following informalities:

The Related Applications section contains significant gaps in the record, as well as information in need of updating. The applicant must fill in all of the blanks, and must show which applications have which status.

Appropriate correction is required.

3. Applicant is required to modify the brief summary of the invention and to restrict the descriptive matter so that they are confined to and in harmony with the invention to which the allowed claims are directed. See MPEP § 1302.01. For example, a portion of the specification, suggested pages 64-217 should be cancelled.

Drawings

4. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the digital certificate features must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate

prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Information Disclosure Statement

5. The information disclosure statement filed 1/8/02 and 2/12/02 fail to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each U.S. and foreign patent; each publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered. In both cases, the Abrash publication is missing from the file, and thus can not be considered.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-2, 15, 18 and 23-24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- a) As to claims 1-2 and 23-24, "the same Subject" and "the Version field" lack antecedent basis.
- b) As to claim 15, "said unsigned integer" lacks antecedent basis.
- c) As to claim 18, "the expiration date" lacks antecedent basis.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-2, 4, 13 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Collins et al. (2002/0038420) in view of Kaliski, Jr. (6,189,098) and further in view of Schneier (Applied Cryptography).

- a) As to claims 1-2 and 24, Collins discloses a method for forming a public key based certificate for mobile and desktop environments comprising using a common data object header in substantially all communicated data including communicated certificates (Fig. 4, elements 404, 408); providing a plurality of public keys including a first public key and a second public key in a single certificate (Abstract; Fig.4, elements

Art Unit: 2137

428, 432); providing a tag field that function as a discriminator of different certificates issued to the same subject (Fig. 4, element 420).

Collins does not disclose each of the first and second public keys being associated with its own purpose.

Kaliski discloses a protocol for establishing the authenticity of a client to a server where the certificate contains two separate keys along with identification as to their purposes (col. 13, lines 59-61).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of associating public keys with its own purpose as Kaliski teaches in the system of Collins so as to specifically include all needed information in the certificate.

Collins and Kaliski do not disclose representing a subject name and an issuer name in one fixed character set determined by the version field.

Schneier discloses the version field identifies the certificate format (X.509 certificate, pages 574-575). Schneier teaches a certificate where subject name and issuer name are the elements and determined by the version field in one fixed character set.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of determining the character set for representing a subject name and an issuer name by the version field as Schneier teaches in the system of Collins and Kaliski so as to specifically include all needed information in the certificate.

b) As to claim 4, Collins discloses the purpose is selected from the group of purposes consisting of encrypting messages, encrypting session keys, signing messages, signing and encrypting data and combinations thereof (page 3, paragraphs [0026, 0028, 0032-0033].

c) As to claim 13, Collins discloses the system parameters include an RSA exponent or Diffie-Helman Generator (page2, paragraph [0021]).

10. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Collins et al. (2002/0038420) in view of Kaliski, Jr. (6,189,098), in view of Schneier (Applied Cryptography), and further in view of Davie et al. (6,430,155).

Collins, Kaliski and Schneier do not disclose the unsigned integer has a four byte value.

Davie discloses the unsigned integer has a four byte value (col. 13, lines 31-32).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of unsigned integer having a four byte value as Davie teaches in the system of Collins, Kaliski and Schneier so as to specifically format the tag field.

11. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Collins et al. (2002/0038420) in view of Kaliski, Jr. (6,189,098), in view of Schneier (Applied Cryptography), and further in view of Generous et al. (2002/0120697).

Collins, Kaliski and Schneier do not disclose the tag field is treated as ASCII characters to represent the expiration date of the certificate.

Generous discloses a system for delivery of a message to a subscriber over multiple communications channels comprising information with expiration formatted in ASCII characters (page 14, paragraph [0487]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of ASCII characters to format the expiration date as Generous teaches in the system of Collins, Kaliski and Schneier so as to specifically format the tag field.

12. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Collins et al. (2002/0038420) in view of Kaliski, Jr. (6,189,098), in view of Schneier (Applied Cryptography), and further in view of Asay et al. (2002/0062438).

Collins, Kaliski and Schneier do not disclose the version field indicate any additional fields that are present in the certificate.

Asay discloses additional fields can be extensions as prescribed in the version (page 27, paragraph [0489]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of version field indicating additional fields as Asay teaches in the system of Collins, Kaliski and Schneier so as to specifically format the version field.

Allowable Subject Matter

13. Claims 3, 5-11, 12, 14, 16-17 and 19-21 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

14. Claim 23 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, second paragraph, set forth in this Office action.

The prior arts of Collins, Kaliski, Schneier, Davie and Generous do not disclose the method of claim 23 where tag field and its elements are implemented.

Conclusion

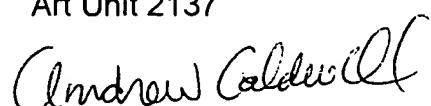
15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER